UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MASSACHUSETTS

DALLAS PERKINS, on behalf of himself and all others similarly situated, Plaintiff, v. **MARRIOTT INTERNATIONAL, INC., and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC**, Defendants.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Dallas Perkins ("Plaintiff"), on behalf of himself and all others similarly situated, files this Class Action Complaint ("Complaint") against Defendants Marriott International Inc., and Starwood Hotels & Resorts Worldwide, LLC (collectively "Marriott" or "Defendants"), and respectfully alleges the following:

NATURE OF THE ACTION

1. This class action seeks to redress Marriott's unlawful and negligent disclosure of millions of consumers' confidential personal identifying information ("PII"), including their names, addresses, passport details, phone numbers, email addresses, dates of birth, gender, and credit card numbers with expiration dates in violation of Massachusetts' consumer protection law, MASS. GEN. LAWS 93A § 1, the consumer protection laws of states with materially identical terms, and common law.

2. Marriott failed to fulfill its legal duty to protect consumers' PII which was stored in its systems. Marriott's willful, reckless, and negligent disregard for its obligations to safeguard individuals' PII resulted in a massive data breach that has been occurring since at least 2014, exposing hundreds of millions of consumers' PII ("Data Breach" or "Breach").

3. Plaintiff brings this action on behalf all persons who reside in the United States whose PII was compromised as a result of the Data Breach, all persons who reside in Massachusetts whose PII was compromised as a result of the Data Breach, and all persons who reside in states with materially identical consumer protection laws to Massachusetts whose PII was compromised as a result of the Data Breach (the "Classes" or "Class Members").

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over Plaintiff's claims pursuant to 28 U.S.C. § 1332(d) (CAFA) because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Marriott's citizenship, and (c) the matter in controversy exceeds $5 million, exclusive of interest and costs.

5. This Court has personal jurisdiction over Marriott because it both intentionally avails itself of the rights and privileges of conducting business in Massachusetts and it has continuous and systematic contacts with Massachusetts owing to Marriott's hotel and lodging locations in Massachusetts and advertising targeting Massachusetts citizens.

6. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

PARTIES

7. Plaintiff Dallas Perkins is a resident of Cambridge, Massachusetts. Mr. Perkins has repeatedly stayed at Starwood-branded properties in the United States and abroad since 2014, including making reservations at and staying at a Starwood-branded W Hotel in Amsterdam in the Spring of 2017 and a W Hotel in Barcelona in or around 2015.

8. Defendant Marriott International, Inc. is incorporated under the laws of the State of Delaware, with its principal place of business in Bethesda, Maryland. Marriott operates through various subsidiaries, each of which acts as an agent of or in concert with Marriott.

9. Defendant Starwood Hotels & Resorts Worldwide, LLC is incorporated under the laws of the State of Maryland, with its principal place of business in Bethesda, Maryland.

FACTS

I. The Marriott Data Breach

10. Marriott is the largest hotel chain in the world, with more than 6,500 properties located in 127 countries and territories globally. Marriott owns and operates a variety of hotel, lodging, and hospitality brands, including hotels under its Starwood brands, which include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels. Hundreds of millions of customers have made reservations and stayed at Marriott properties around the globe.

11. When booking reservations at a Marriott property, including its Starwood brand properties, customers provide Marriott with sensitive PII, including their names, addresses, passport numbers and details, phone numbers, email addresses, dates of birth, gender, and credit card numbers with expiration dates.

12. Booking hotel reservations, and thus, collecting the PII of its customers, is therefore at the heart of Marriott's business.

13. Moreover, individuals who entrust Marriott with PII, which includes extremely sensitive data such as passport details and credit card information, do so with the understanding that Marriott will safeguard that information. That expectation is directly reinforced by Marriott, which publicly touts its commitment to safeguarding customers PII, including for example in its Marriott Group Global Privacy Statement, where it purports to "use reasonable organizational,

technical and administrative measures to protect Personal Data."[1] Likewise, Defendants' Marriott U.S. Privacy Shield Guest Privacy Policy represents to customers that it will "use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction."[2]

14. Despite these promises that it is committed to safeguarding guests' PII, in a November 30, 2018 statement, Marriott revealed that data for approximately 500 million guests was exposed in a hack that has allowed unauthorized access to its Starwood Hotels reservation database since 2014, and that hackers have actively copied and encrypted information from this database.[3]

15. The statement further revealed that Defendant initially discovered the Breach months earlier, on September 8, 2018.[4]

16. The Breach compromised "some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences" for at least 327 million individuals, and names, mailing addresses and unidentified "other information" for at least 150 million other individuals.[5]

17. At this time, it is unclear why the Breach was not discovered for four years, or why it took over two-and-a-half months for Marriott to verify and report the Breach to the

---

[1] *See* https://www.marriott.com/about/privacy.mi (last accessed Nov. 30, 2018).

[2] *See* https://www.marriott.com/about/global-privacy.mi (last accessed Nov. 30, 2018).

[3] *See Marriott Announces Starwood Guest Reservation Database Security Incident*, MARRIOTT NEWS CENTER (Nov. 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last accessed Nov. 30, 2018).

[4] *See id.*

[5] *See id.*

victims whose PII had been stolen. Such a delay is damaging to the Breach's victims, in that they could have immediately acted in a manner to protect themselves and their PII from further harm.

18. As Marriott's President and Chief Executive Officer Arne Sorenson has admitted, "[Marriott] fell short of what our guests deserve and what we expect of ourselves" in allowing this Breach to occur.[6]

II. Data Breaches Lead To Identity Theft.

19. Data thieves intentionally hack into inadequately protected servers to steal PII with the primary incentive of weaponizing that private data to commit identity theft and financial fraud. Identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.

20. Given the scope of this Breach and the nature of the PII compromised, the ways in which criminals may unlawfully use the data is limitless, as is the timeframe for using the information for criminal endeavors.

21. Unfortunately for Plaintiff and the Classes, a person whose PII has been compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

---

[6] *See id.*

[7] G.A.O., PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (June 2007), http://www.gao.gov/assets/270/262904.html.

22. The information implicated in the instant Breach is particularly susceptible to delay tactics in that an individual's name, address, passport number, and Social Security number are not easily changed to mitigate risk over time. Accordingly, Plaintiff and the Class Members will bear a heightened risk of identity theft or fraud for the unforeseeable future.

23. Identity theft occurs when an individual's PII is used without his or her permission to commit fraud or other crimes.[8]

24. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[9]

25. As a direct and proximate result of Marriott's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII, Plaintiff and the Classes are susceptible to identity theft.

26. The risks associated with identity theft are serious. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, banking or finance fraud, and government fraud. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job

[8] *See* FEDERAL TRADE COMMISSION: TAKING CHARGE: WHAT TO DO IF YOUR IDENTITY IS STOLEN (April 2013), https://www.consuer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[9] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (March 2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[10]

27. Having obtained the Plaintiff and Class Members' names, addresses, passport details, phone numbers, email addresses, dates of birth, gender, and credit card numbers and expiration dates, cybercriminals can simply use the data revealed or pair the data with other available information to commit a broad range of fraud in an victim's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing fraudulent tax returns;
- obtaining medical care and filing prescriptions;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public documents.

28. Passport data was also included in the breach. Passports are considered to be one of the most powerful travel documents in the world.

29. Having obtained the Plaintiff and Class Members' passports, cybercriminals can use the data to commit a broad range of fraud in an victim's name, including opening bank accounts, and illegally entering the country and masking their identity from the authorities.[11]

[10] TRUE IDENTITY PROTECTION: IDENTITY THEFT OVERVIEW, http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf (visited Sept. 23, 2016).

[11] Gabriel Wood, *Common Forms of ID Criminal Use to Commit Identity Theft, available at* https://www.nextadvisor.com/blog/common-forms-of-id-criminals-use-to-commit-identity-theft/

30. Beyond using the data exposed for nefarious purposes themselves, the cybercriminals who obtained Plaintiff and Class Members' PII may also exploit the data by selling it on the "black market" or "dark market" for years following a breach.

31. Indeed, there is a well-established international black market where hackers may quickly and efficiently sell -- in part or in whole -- precisely the type of PII stolen in the instant Data Breach.

32. Moreover, much like regular online marketplaces (such as eBay), many dark market websites (such as AlphaBay) include feedback systems for vendors, refund policies, and easily navigable search categories.[12]

33. The PII exposed in the Breach, which included, *inter alia*, names, birth dates, addresses, and Social Security numbers, qualifies as what hackers and black markets term as "fullz" records.[13] According to one 2015 estimate, the median price for someone's identity on the black market is approximately $21.35.[14] Fullz records are notably on the higher end of the pricing spectrum because they entail a "full set" of individuals' PII and the range of PII sold in the same markets also includes less glamorous information, such as basic credit card information.

34. Cybercriminals can further post stolen PII on the internet, thereby making such information publically available.

---

[12] Keith Collins, *Here's what your stolen identity goes for on the internet's black market*, QUARTZ, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

[13] Brian Feldman, *So What Happens With All That Equifax Data?*, N.Y. MAGAZINE, Sept. 8, 2017, http://nymag.com/selectall/2017/09/so-what-happens-with-all-that-equifax-data.html.

[14] Keith Collins, *Here's what your stolen identity goes for on the internet's black market*, QUARTZ, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

35. Moreover, individuals whose PII is subject to a reported security breach -- such as the Data Breach at issue here -- are approximately 9.5 times more likely than the general public to suffer identity fraud or identity theft.[15]

III. Marriott Was On Notice Of The Risks Of Cybersecurity Attacks.

36. Marriott was well aware of the risk of cybersecurity attacks and data breaches.

37. Data security breaches -- and data security breach litigation -- dominated the headlines in recent years, including into 2018.[16] According to the Privacy Rights Clearinghouse Chronology of Data Breaches, over 1,300 breaches were publicly reported in 2017 and 2018 alone.[17]

38. The hospitality industry has become a main target of cyber-attacks. Many other hospitality chains have had major PII breaches. Since the hospitality industry has become a target for attackers, Marriott was clearly aware of this threat.[18]

---

[15] See Javelin Strategy & Research, *Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier*, *available at* https://www.javelinstrategy.com/news/1314/92/1 (last visited Jun. 16, 2014).

[16] *See e.g.*, Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN Tech (Sept. 23, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/; Sara Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could Be Affected*, CNN Tech (Sept. 8, 2017), https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html; Jim Finkel and David Henry, *Saks, Lord & Taylor Hit By Payment Card Data Breach*, Reuters (Apr. 3, 2018), https://www.reuters.com/article/legal-us-hudson-s-bay-databreach/saks-lord-taylor-hit-by-payment-card-data-breach-idUSKCN1H91W7; Bill Hutchinson, *87 million Facebook Users To Find Out If Their Personal Data Was Breached*, ABC News (Apr. 9, 2018), https://abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187.

[17] *See* Privacy Rights Clearinghouse Chronology of Breaches *available at* http://www.privacyrights.org.

[18] See Hospitality Technology, *Cybersecurity Tactics for a Hotel Industry that's Under Siege*, *available at* https://hospitalitytech.com/cybersecurity-tactics-hotel-industry-thats-under-siege (last visited Nov. 30, 2018).

39. For instance, in its SEC filings, Marriott stated that "Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years."[19]

40. Furthermore, this is not the first time the company has faced a data breach. Rather, Marriott -- specifically at its Starwood properties -- has acknowledged or been implicated in previous data breach in 2016.[20]

IV. Plaintiff And Class Members Suffered Damages As A Result Of The Data Breach.

41. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiff and Class Members' PII against reasonably foreseeable threats to the security or integrity of such information.

42. Marriott failed to identify, implement, maintain, and monitor appropriate data security measures, polices, procedures, controls, protocols, and software and hardware systems to ensure the security of Plaintiff and Class Members' PII.

43. Additionally, Plaintiff and Class Members' PII was improperly handled, stored, segregated, and in some cases, either unencrypted or improperly partially encrypted, inadequately protected, readily able to be copied by data thieves, and not kept in accordance with basic security protocols. Indeed, Marriott itself conceded that only credit card data was encrypted.[21]

---

[19] Marriott International Inc., Annual Report (Form 10-K) (Feb. 15, 2018).

[20] Alwyn Scott, Starwood, *Marriott, Hyatt, IHG hit by malware: HEI*, REUTERS, Aug. 14, 2016, https://www.reuters.com/article/us-hotels-cyber/starwood-marriott-hyatt-ihg-hit-by-malware-hei-idUSKCN10P0ZM.

[21] *See Marriott Announces Starwood Guest Reservation Database Security Incident*, MARRIOTT NEWS CENTER (Nov. 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last accessed Nov. 30, 2018).

44. Had Marriott taken appropriate security measures, the Data Breach would not have occurred.

45. Marriott's wrongful actions, inactions, and omissions directly and proximately caused the theft of Plaintiff and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harms for which they are entitled compensation, including, *inter alia*:

a. actual or attempted identity theft or fraud;

b. increased risk of harm, including actual identity theft and fraud;

c. the untimely and inadequate notification of the Data Breach;

d. improper disclosure of their PII;

e. diminution in the value of their PII;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of identity theft, identity fraud, and medical fraud;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to mitigate or avert the increased risk of identity theft, identity fraud, and medical fraud;

46. Moreover, consumers value data security and are willing to pay more for services that come with data security. It is for this reason that Marriott goes to such lengths to assure customers that their PII is safe.

47. Studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49–44.62."[22] When consumers

[22] *See* Il-Horn Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2002), http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (emphasis added); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) INFORMATION SYSTEMS RESEARCH 254, 254 (June 2011).

were surveyed regarding how much they value their PII in terms of its protection against improper access and unauthorized secondary use—the very concerns at issue here—they valued the restriction of improper access to their data at between $11.33 and $16.58 per website, and prohibiting secondary use to between $7.98 and $11.68 per website.[23]

48. To date, Marriott has not offered Plaintiff and Class Members any compensation from the past, present, and future harm they may experience as a result of the Data Breach.

CLASS ACTION ALLEGATIONS

49. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and all other similarly situated individuals within the United States (the "Nationwide Class"), defined as follows:

> All persons who reside in the United States whose PII was compromised as a result of the Data Breach.

50. Additionally, Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and all other similarly situated individuals within the state of Massachusetts (the "Massachusetts Class"), defined as follows:

> All persons who reside in Massachusetts whose PII was compromised as a result of the Data Breach.

51. Additionally Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of himself and all other similarly situated individuals within certain States (the "Multi-State Class"), defined as follows:

> All persons who reside in California, Florida, Illinois, Massachusetts, Michigan, New Jersey, New York, North Carolina, Ohio, and Washington whose PII was compromised as a result of the Data Breach.

[23] *Id.*

52. Plaintiff reserves the right to modify or amend the Class definitions before the court determines whether class certification is appropriate.

53. Excluded from all of the above Classes are: (i) Defendant and any entities in which Defendant has a controlling interest; (ii) any entities in which Defendant's officers, directors, or employees are employed and any of the legal representatives, heirs, successors, or assigns of Defendant; (iii) the Judge to whom this case is assigned and any member of the Judge's immediate family and any other judicial officer assigned to this case; and (iv) all governmental entities.

54. The members of the Class are so numerous that their joinder is impracticable. According to Marriott, there are hundreds of millions of Class Members. Their identities, phone numbers, home addresses, and email addresses can be easily derived from Marriott's internal (and now external) records.

55. The rights of the Plaintiff and each Class Member were violated in precisely the same manner by Marriott's reckless and negligent actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of their PII.

56. There are questions of law and fact common to the Class, as a whole. The common questions of law and fact predominate over any questions affecting only individual Members of the Class, and include, without limitation:

a. Whether Marriott had a duty to protect the Plaintiff and the Class Members' PII;

b. Whether Marriott breached it duty to protect the Plaintiff and the Class Members' PII;

c. Whether Marriott's breach of a legal duty caused its systems to be compromised, resulting in the loss and/or potential loss of approximately 500 million individuals' PII;

d. Whether Marriott properly designed, adopted, implemented, controlled, managed, and monitored data security processes, controls, policies, procedures and/or protocols to protect Plaintiff's and the Class Members' PII in the Data Breach;

e. Whether Marriott failed to timely inform Plaintiff and the Class Members of the Data Breach;

f. Whether Marriott's conduct was willful;

g. Whether Marriott's conduct was negligent; and

h. Whether Plaintiff and Class Members are entitled to damages.

57. Plaintiff's claims are typical of the claims of the Class Members because Plaintiff, like all Class Members, is a victim of Marriott's wrongful actions, inaction, and omissions that caused the Data Breach, caused the unauthorized release and disclosure of his PII. Plaintiff and his counsel will fairly and adequately represent the interests of the Class Members. Plaintiff has no interests antagonistic to, or in conflict with, other Class Members' interests. Plaintiff's counsel is highly experienced in the prosecution of complex commercial litigation, consumer class actions, and data breach cases.

58. A class action provides a fair and efficient method, if not the only method, for adjudicating this controversy. The substantive claims of the representative Plaintiff and the Classes are nearly identical and will require evidentiary proof of the same kind and application of the same law. There is no plain, speedy or adequate remedy other than by maintenance of this class action.

59. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class Members number in the millions and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed Class Members to prosecute their claims individually. Trial of Plaintiff's and the Class Members' claims is manageable. Unless the Class is certified,

Defendant will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

60. Certification of the Class, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

61. Certification of the Class, also is appropriate under FED. R. CIV. P. 23(b)(2) because Marriott has acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

62. Certification of the Class, also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Equifax.

63. Marriott's wrongful actions, inaction, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiff also seeks equitable remedies for the Class.

64. Marriott's systemic policies and practices also make injunctive relief for the Class appropriate.

65. Absent a class action, Marriott will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiff and Class Members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence On Behalf Of The Nationwide Class

66. Plaintiff re-alleges and incorporate by reference all preceding factual allegations as though fully set forth herein.

67. Plaintiff bring this claim on behalf of himself and the Nationwide Class.

68. Equifax had a duty to Plaintiff and Class Members to safeguard and protect their PII.

69. Defendant assumed a duty of care commensurate with industry standards to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

70. Defendant had full knowledge about the sensitivity of Plaintiff and Class Members' PII, the PII's value to criminals, the increasing prevalence of data breaches, as well as the type of harm to could occur if such PII was wrongfully disclosed.

71. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

72. Defendant had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with such highly sensitive PII data.

73. Defendant breached its duty of care by failing to secure and safeguard the PII of Plaintiff and Class Members. Defendant negligently stored and/or maintained its systems.

74. Further, Defendant, by and through its above negligent actions and/or inaction, further breached its duties to Plaintiff and Class Members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff and Class Members' PII within its possession, custody and control.

75. Plaintiff and Class Members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised PII subjects each of them to a

greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

76. It was reasonably foreseeable -- in that Defendant knew or should have known -- that its failure to exercise reasonable care in safeguarding and protecting Plaintiff and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

77. But for Defendant's negligent and wrongful breach of its responsibilities and duties owed to Plaintiff and Class Members, their PII would not have been compromised.

78. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm -- for which they are entitled to compensation. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

79. Plaintiff and Class Members are entitled to injunctive relief as well as actual and punitive damages.

SECOND CAUSE OF ACTION
Invasion of Privacy On Behalf Of The Nationwide Class

80. Plaintiff re-alleges and incorporate by reference all preceding factual allegations as though fully set forth herein.

81. Plaintiff bring this claim on behalf of himself and the Classes.

82. Plaintiff and Class Members' PII is private information.

83. Dissemination of Plaintiff and Class Members' PII would be offensive to a reasonable person.

84. The public has no legitimate interest in being apprised of Plaintiff and Class Member's PII.

85. Defendant's failure to safeguard and protect Plaintiff and Class Members' PII directly and proximately resulted in unreasonable publicity to the private lives of Plaintiff and Class Members.

86. Plaintiff and Class Members' have a legal interest in the privacy of their PII.

87. Defendant's failure to safeguard and protect Plaintiff and Class Members' PII was a direct and proximate cause of the access to the PII and the obtaining of the PII as a matter of law.

88. Defendant's failure to safeguard and protect Plaintiff and Class Members' PII deprived Plaintiff and Class Members of their legal interest in the privacy of that information, causing them damages.

89. As a result of Defendant's actions and inactions resulting in Plaintiff and Class Members' loss of privacy, Plaintiff and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described above.

THIRD CAUSE OF ACTION
Violation of MASS. GEN. LAWS 93A § 1 *et seq.* On Behalf Of The Massachusetts Class

90. Plaintiff Perkins re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

91. Plaintiff Perkins brings this claim on behalf of himself and the Massachusetts Class.

92. MASS. GEN. LAWS 93A § 2(a) declares unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

93. Defendant engaged in false and misleading representations to the public and to consumers (*i.e.*, individuals and entities seeking its services) concerning its data security in order to be entrusted with highly sensitive PII, which it received from a variety of sources including financial institutions, and in order to benefit financially.

94. In the course of Defendant's trade or commerce, it willfully failed to disclose that its cybersecurity systems were inadequately protected and that its cybersecurity policies and procedures were inadequately implemented. In turn, Defendant willfully made affirmative representations that individuals' PII would be safe in its hands.

95. Furthermore, Defendant failed to timely disclose the Breach to Plaintiff and Class members; indeed, Equifax has known for well over a month that the data was compromised.

96. Accordingly, Defendant made untrue, deceptive, and misleading representations of material facts and omitted and concealed material facts to the public, consumers, Plaintiff, and the Class.

97. In reality, Defendant failed to provide adequate protection for Plaintiff's and Class Members' PII, resulting in the Breach.

98. The security of Defendant's data systems was a material fact to Plaintiff and the Class. Had the public known of Defendant's misrepresentations and omissions as described herein, Defendant would not have been entrusted with the PII it has since compromised.

99. Plaintiff and the Class sustained (and continue to sustain) injuries and damages caused by Defendant's affirmative statements, as well as its failure to disclose material information, as described above.

100. Accordingly, Plaintiff, on behalf of himself and the Class Members, respectfully request this Court award all relevant damages for Equifax's unfair methods of competition, and unfair and deceptive practices.

FOURTH CAUSE OF ACTION
Violation Of Materially Identical State Consumer Protection Statutes On Behalf Of The Multi-State Class

101. Plaintiff incorporates by reference and realleges herein all paragraphs alleged above.

102. Marriott is engaged in "trade" and "commerce" as it markets and provides accommodations at its hotels and lodgings to consumers.

103. Marriott's false representations regarding the security measures it uses to protect consumers' PII was material to a reasonable consumer and likely to affect consumer decisions and conduct.

104. Marriott has used and employed unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce.

105. Marriott's acts and practices are immoral, unethical, oppressive and unscrupulous.

106. Marriott's conduct is substantially injurious to consumers. Such conduct has, and continues to cause, substantial injury to consumers because consumers would not have provided Marriott with their PII had Marriott not made false representations as to its data security measures. Consumers were thus injured when Marriott allowed their PII to be stolen by cybercriminals in the Data Breach and such injury is not outweighed by any countervailing benefits to consumers or competition.

107. No benefit to consumers or competition results from Marriott's conduct. Since reasonable consumers are deceived by Marriott's representations of its data security and they were injured as a result, consumers could not have reasonably avoided such injury.

108. The foregoing unfair and deceptive practices directly, foreseeably and proximately caused Plaintiff and the Multi-State Class to suffer an ascertainable loss when Marriott allowed their PII to be stolen by cybercriminals.

109. The practices discussed above all constitute unfair competition or unfair, unconscionable, deceptive, or unlawful acts or business practices in violation of at least the following state consumer protection statutes:[24]

a. **California Consumer Legal Remedies Act,** Cal. Civ. Code § 1750, *et seq*.,

b. **California Unfair Competition Law,** Cal. Bus. & Prof. Code § 17200, *et seq*.;

c. **Florida Deceptive and Unfair Trade Practices Act,** Fla. Stat. § 501.201, *et seq.*;

d. **Illinois Consumer Fraud and Deceptive Business Practices Act**, 815 Ill. Comp. Stat. § 505/1, *et seq.*;

e. **Massachusetts Regulation of Business Practices for Consumers' Protection Act**, Mass. Gen. Laws Ann. ch. 93A, § 1 *et seq.*;

f. **Michigan Consumer Protection Act,** Mich. Comp. Laws § 445.901 *et seq.*;

g. **New Jersey Consumer Fraud Act**, N.J. Stat. Ann. § 56:8-1, *et seq*.;

h. **New York Deceptive Acts and Practices Act**, N.Y. Gen. Bus. Law § 349, *et seq.*;

i. **North Carolina Unfair and Deceptive Trade Practices Act,** N.C. Gen. Stat. § 75-1.1(a).

j. **Ohio's Consumers Sales Practice Act,** Ohio Revised Code § 1345, *et seq*.

k. **Washington Consumer Protection Act**, Wash. Rev. Code § 19.86.010, *et seq.*;

[24] There is no material conflict between these state statutes because these state statutes (1) do not require reliance by unnamed class members; (2) do not require scienter; and (3) allow class actions.

110. The foregoing unfair and deceptive practices directly, foreseeably and proximately caused Plaintiff and the Multi-State Class to suffer an ascertainable loss when their PII was stolen.

111. Plaintiff and the Multi-State Class are entitled to recover damages and other appropriate relief, as alleged below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Classes pray for judgment as follows:

A. For an Order certifying the proposed Classes pursuant to FED. R. CIV. P. 23(b)(1), (2) and/or (3), appointing Plaintiff as Class Representative for each Class, and appointing Greg Blankinship of FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP as Class Counsel;

B. For appropriate injunctive relief and declaratory relief, including an order requiring Defendant to immediately secure and fully encrypt all confidential information, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing confidential information, and to provide identity theft monitoring for an additional five years;

C. Adjudging and decreeing that Defendant has engaged in the conduct alleged herein;

D. For compensatory and general damages according to proof on certain causes of action, as well as injunctive relief, and statutory, actual, and other applicable damages, including punitive damages;

E. For reimbursement, restitution and disgorgement on certain causes of action;

F. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

G. For costs of the proceedings herein;

H. For an Order awarding Plaintiff and the Classes reasonable attorneys' fees and expenses for the costs of this suit; and

I. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand trial by jury of all claims and causes of action in this lawsuit to which they is so entitled.

Dated: November 30, 2018

Respectfully submitted,

By: */s/ D. Greg Blankinship*

D. Greg Blankinship
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP.
445 Hamilton Ave, Suite 605
White Plains, New York 10601
Telephone: (914) 298-3281
Fax: (914) 908-6709
gblankinship@fbfglaw.com

Daniel S. Robinson
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Drive
Newport Beach, California 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292
drobinson@robinsonfirm.com

Counsel for Plaintiff and the Classes